

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

INVENTORS: Douglas M. Grover
Douglas Steck
W. Paul Willes
Thomas R. Rohlfing
Ronald S. Leahy

ASSIGNEE: Phonex Broadband Corporation

SERIAL NUMBER: n/a

DATE FILED: n/a

TITLE: A METHOD AND APPARATUS FOR A PER-PACKET ENCRYPTION
SYSTEM

ATTORNEY DOCKET: 4492 P

Mail Stop: PATENT APPLICATION
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

COVER LETTER

Honorable Commissioner:

Enclosed herewith please find the following documents comprising a United States patent application: (1) specification, claims and drawings, (2) declaration of inventor(s), (3) fee calculation sheet, (4) fee, (5) statements of small entity status, (6) information disclosure statement and form(s) 1449, (7) assignment and recordation of assignment cover sheet, and (8) return receipt postcard.

Respectfully submitted this 11th day of February, 2004.



Lloyd W. Sadler, Reg. No. 40,154
PARSONS BEHLE & LATIMER
201 South Main Street, Suite 1800
Salt Lake City, Utah 84111
Telephone: (801) 532-1234
Facsimile: (801) 536-6111

Express Mailing
Label:
ER509040615US

SPECIFICATION

[Electronic Version 1.2.8]

A METHOD AND APPARATUS FOR A PER-PACKET ENCRYPTION SYSTEM

Background of Invention

[0001] Field of the Invention. This invention relates to electronic communications systems. More specifically, this invention relates to electronic communications systems which encrypt packets.

[0002] Description of Related Art. A variety of communication systems use methods for encrypting packets as they are sent across a network. Typically, such approaches do not allow for flexible per-packet encryption based on fields in the packets to isolate networks and communications within a network. Although these references may not constitute prior art, for general background material, the reader is directed to the following United States Patents, each of which is hereby incorporated by reference in its entirety for the material contained therein: U.S. Patent Numbers: 6,415,031, 6,253,326, 6,185,680, 6,092,191, 6,052,466, 5,898,784, 5,805,705, and 5,594,869.

Summary of Invention

[0003] It is desirable to provide a packet encryption system that can encrypt or not encrypt each packet based on specific elements of the packet's content, thus providing isolation and securing for specific applications, networks, sub-networks, nodes, protocols, etc.

[0004] Therefore it is a general object of this invention to provide a packet encryption system that can provide per-packet encryption based on one or more different encryption keys.

[0005] It is a further object of an embodiment of this invention to provide a per-packet encryption system based an encryption key identifier within a packet or group of packets.

[0006] It is a further object of an embodiment of this invention to provide a per-packet encryption system based on information within the packet or information external to the packet.

[0007] It is a further object of an embodiment of this invention to provide a per-packet encryption system based a node address.

[0008] It is a further object of an embodiment of this invention to provide a per-packet encryption system based a network address.

[0009] It is a further object of an embodiment of this invention to provide a per-packet encryption system that can encrypt packets based on a sub-network address.

[0010] It is a further object of an embodiment of this invention to provide a per-packet encryption system that can encrypt packets based on a socket.

[0011] It is a further object of an embodiment of this invention to provide a per-packet encryption system that can encrypt packets based upon the protocols within each packet.

[0012] It is a further object of an embodiment of this invention to provide a per-packet encryption system based on any field within the Open System Interconnect model.

[0013] It is a further object of an embodiment of this invention to provide a per-packet encryption system based any combination of fields within the packet payload.

[0014] It is a further object of an embodiment of this invention to provide a packet decryption system that can provide per-packet decryption based on different encryption keys.

[0015] It is a further object of an embodiment of this invention to provide a per-packet decryption system based an encryption key identifier within a packet or group of packets.

[0016] It is a further object of an embodiment of this invention to provide a per-packet encryption and decryption system using a communication channel on a wireless network, a power line network, a light frequency network, an acoustic network and a wired network.

[0017] These and other objects of this invention will be readily apparent to those of ordinary skill in the art upon review of the following drawings, detailed description, and claims. In the present preferred embodiment of this invention, the per-packet encryption system makes use of a novel packet encryption scheme based on an encryption key identifier placed in the packet or within a group of packets.

Brief Description of Drawings

[0018] In order to show the manner that the above recited and other advantages and objects of the invention are obtained, a more particular description of the preferred embodiments of this invention, which are illustrated in the appended drawings, is described as follows. The reader should understand that the drawings depict only

present preferred and best mode embodiments of the invention, and are not to be considered as limiting in scope. A brief description of the drawings is as follows:

[0019] Figure 1a is a diagram of the present preferred network for sending packets between network nodes.

[0020] Figure 1b is a diagram of the present preferred encryption packet structure used by this invention.

[0021] Figure 2 is a diagram of another present preferred encryption packet structure used by this invention.

[0022] Figure 3 is a flow diagram of the present preferred encryption key and encryption key identifier exchange process.

[0023] Figure 4 is a flow diagram of the present preferred packet encryption process for a node sending packets on a network.

[0024] Figure 5 is a flow diagram of the present preferred packet decryption process for a node receiving packets on a network.

[0025] Figure 6 is a flow diagram of the present preferred packet encryption process for sending packet groups.

[0026] Figure 7 is a flow diagram of the present preferred packet encryption process for receiving packet groups.

[0027] Reference will now be made in detail to the present preferred embodiment of the invention, examples of which are illustrated in the accompanying drawings.

Detailed Description

[0028] Figure 1a is a diagram of the present preferred network for sending packets between network nodes. A communication channel 152 is formed by a sending network node 150 and receiving network node 151 which send packets 103 or packet groups 205 between the network nodes.

[0029] Figure 1b is a diagram of the present preferred encryption packet structure used by this invention. Packets 103 are constructed on a sending network node 150 and sent across a communication channel 152 using an encryption key identifier field 100, a destination address field 101, and packet data 102. The payload 104 is defined as anything in the packet other than the encryption key identifier. The destination address field 101 is used to identify a single node or a plurality of nodes on the network. For example, the destination address field 101 can be a broadcast to all nodes on the network or a sub-net address which address specific nodes within the network.

The destination address field 101 can also be a network address used to identify a node or nodes on a remote network. The encryption key identifier field 100 is used to identify an encryption key 105 used to encrypt the packet payload 104 or parts of the packet payload 104 such as only encrypting the data 102 portion of the packet. The encryption key identifier field 100 can also be used to indicate that the packet payload 104 is not encrypted. The packet payload 104 gets encrypted using the encryption key 105 pointed to by the encryption key identifier field 100. The whole packet payload 104 can be encrypted and the packet 103 can be sent without addressing on a point-to-point network. When the packet is received in the receiving network node 151 the encryption key identifier field 100 is used to select the associated encryption key 105 and decrypt the packet.

[0030] Figure 2 is a diagram of another preferred encryption packet structure used by this invention. Packets 200–202 are constructed on a sending network node 150 and sent across a communication channel 152 in packet groups 205. One of the packets 200 contains an encryption key identifier 203 used for encryption of the payload fields 204, 201, 202 of all packets in the packet group 205. As shown in figure 2, packet one 200 contains the encryption key identifier 203 and optionally a payload field 204. Packets two 201 and subsequent packets 202 are encrypted using the encryption key identifier's 203 encryption key or keys 206. The order in which the packets 200–202 are sent is not critical to decrypting the packet group 205 as long as at least one packet

200–202 in the packet group 205 contains the encryption key identifier 203. The packet group 205 is received by the receiving network node 151. The receiving network node 151 uses the encryption key identifier 203 and encryption key 206 to decrypt the packet group 205.

[0031] Figure 3 is a flow diagram of the present preferred encryption key and encryption key identifier exchange process. It should be noted that some encryption algorithms use multiple encryption keys to encrypt data. The process of passing, encrypting and decrypting can be used with either single encryption key algorithms or multiple encryption key algorithms. The present preferred embodiment uses Diffie–Hellman key exchange to exchange encryption keys and encryption key identifiers, but many other alternative key exchange processes will work. The process starts 300 with a user, application, or an external input setting up criteria 301 for the per–packet encryption process. The criteria used can be any field or combination of fields within the packet payload 104, 201, 202, 204 such as without limitation the node address, a network address, sub–network address, a socket, a protocol identifier, a service type, and the like. In addition, it can be a criterion passed down from an application or user which is not contained within the packet payload 104, 201, 202, 204. The encryption key 105, 206 (or keys for multiple key encryption algorithms) is exchanged 302 with the nodes on the network that need the encryption key. If 303 this is successful, the application or user is notified 304 of the successful encryption passing process. The

process is complete 307. Otherwise, if test 303 is not successful, the application or user is notified 305 that the encryption passing process failed. If in test 306 the process wants to be tried again, the same key exchange step 302 is repeated. Otherwise, the process is completed 307. Test 306 can be done by a user or alternatively by a process responsible for the system.

[0032] Figure 4 is a flow diagram of the present preferred packet encryption process for a node sending packets on a network. The process starts 400 when there is a packet 103, to send. The sending network node 150 first checks 401 to see if the packet 103 matches the criteria defined for packet encryption. The criteria for encryption can be that the packet payload 104 uses a particular Internet Protocol Address or Service Type or a combination of both. Alternate criteria include, but may not be limited to source or destination network addresses, sub-network addresses, protocol identifiers, source or destination node addresses, application layer information, or any other fields within the packet. Typically, the user or application sets up a grouping of criteria for which a specific encryption key will be used. A criteria group can be one specific criterion or multiple criteria. There can be multiple groups of criteria with an associated encryption key for each group of criteria. If 401 there is a match for the encryption criteria group, the node gets 402 the encryption key associated with the criteria group. The packet payload 104 is encrypted 403 using the encryption key 105. The encryption key identifier field 100 is set in block 404 with the associated encryption key identifier. The

packet 103 is sent 405 from the sending network node 150 across the communication channel 152 along with the encryption key identifier field 100 and the encrypted packet payload 104 or data 102. Otherwise, if the packet does not match any encryption criteria in test 401, the packet encryption identifier field 100 is set 407 to the no encryption value. The packet 103 is sent 408 along with the encryption key identifier 100 for unencrypted packets and the unencrypted packet payload 104. In addition, if only the data 102 portion of the packet 103 is encrypted, the packet can be sent using the destination address field 101 so that the receiving network node 151 does not have to decrypt the payload 104 to determine if the packet 104 is for the receiving network node 151.

[0033] Figure 5 is a flow diagram of the present preferred packet decryption process for a node receiving packets on a network. The process starts 500 with the receiving 501 of a packet. The receiving network node 151 checks to see if the packet is for the receiving network node 151 in test 502. If the packet is not for the receiving network node 152, the process starts over when another packet is received 501. Otherwise, if test 502 is successful, the encryption key identifier is checked 503 to see if the encryption key identifier matches any of the encryption key identifiers stored in the receiving network node's 151 non-volatile memory. If there is a match in test 503, the node gets 505 the encryption key associated with the encryption key identifier. This encryption key is used to decrypt 506 the packet payload. The unencrypted packet data

is passed 507 to the upper protocol layer for processing and the process completes 508. Otherwise, if test 503 is not successful, test 504 checks to see if the encryption key identifier is set to the no encryption value. If not, the process ignores the packet and waits for another packet to be received 501. If the encryption key identifier in test 504 is set to the no encryption value, the packet data is passed 507 to the next protocol layer. The process is complete 508.

[0034] Figure 6 is a flow diagram of the present preferred packet encryption process for sending packet groups. A packet group 205 is one or more packets 200, 201, 202 that have at least one packet 200 which contains the encryption key identifier 203. The process begins 600 when a sending network node 150 has a packet group 205 to send. If in test 601 the packets 200, 201, 202 do not match the criteria to encrypt the packets 200, 201, 202, the encryption key identifier 203 in the packet 200 is set 611 to no encryption and the packet 200 is sent 612. The process is complete 610. Otherwise, if there is a match in test 601, the encryption key 206 which matches the defined criteria is retrieved 602. The first packet 200 is encrypted 603 using the encryption key 206 if it contains a data field or payload 204 to be encrypted. The first packet 200 can only be the key and have no payload or data to encrypt. Having the first packet 200 contain the encryption key identifier 203 is not a requirement as long as it can be identified from other packets 201, 202 within the packet group 205. The encryption key identifier 203 is set 604 to match the corresponding encryption key. The packet 200 is sent 605 with

the encryption key identifier 203. The rest of the packets 201, 202 are sent in the next packet 606. Each of the packets 201, 202 data fields or payloads 201, 202 are encrypted 607 using the encryption key 206 and sent 608. A test is made to determine if 609 there are more packets in the packet group 205. If so the process repeats with the next packet 606. Otherwise, the process completes 610.

[0035] Figure 7 is a flow diagram of the present preferred packet encryption process for receiving packet groups. The process begins 700 upon the receipt 701 of a packet. If in test 702 the packet is not for the receiving network node 151, the process starts over 701. Otherwise, test 703 checks to see if it is the first packet 200 in the packet group 205. If it is the first packet 200, test 704 checks if the encryption key identifier 203 matches any of the stored encryption key identifiers (including the no encryption key identifier). If the encryption key identifier 203 does not match any of the encryption identifiers from test 704 the process starts again with the receipt of a packet 701. Otherwise, test 705 is performed to see if the encryption identifier 203 is set to no encryption. If so, the packet is passed 711 to the next protocol layer and the process starts all over again with the receipt of a packet 701. If test 705 is no, the node gets 708 the encryption key 206 associated with the encryption key identifier 203. This key is used to decrypt 709 the packet payload 204 if there is one. The encryption key 206 is stored 710 in order to be used to decrypt the rest of the packet group 205. The packet is passed 711 to the next protocol layer and the process repeats 701 with the receipt of

a packet. If the received packet is not the first packet 200 in test 703, the received packet is checked 706 based on the stored encryption key identifier which indicates no encryption to see if the packet group 205 is encrypted. If the packet group 205 is not encrypted, the packet is passed 711 to the next protocol layer and the process repeats 701 with the receipt of a packet. Otherwise, the packet is decrypted 707 using the stored encryption key 206 from step 710.

[0036] Since these encryption methods are designed to be physical layer independent, they will run over a wide variety of networks, including but are not limited to such types of networks as AC power line, DC power line, light frequency (fiber, light, or the like), Radio Frequency (RF) networks (wireless such 802.11b, infrared, or the like), acoustic networks and wired (coax, twisted pair, or the like).

[0037] In addition, these data transportation methods can be implemented using a variety of processes, including but are not limited to computer hardware, microcode, firmware, software, or the like.

[0038] The described embodiments of this invention are to be considered in all respects only as illustrative and not as restrictive. Although specific flow diagrams and packet formats are provided, the invention is not limited thereto. The scope of this invention is, therefore, indicated by the claims rather than the foregoing description. All

changes, which come within the meaning and range of equivalency of the claims, are to be embraced within their scope.